KEAMANAN JARINGAN

OLEH :

ERLANGGA IBRAHIM

672017277

TEKNIK INFORMASI

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN SATYA WACANA

SALATIGA

2018

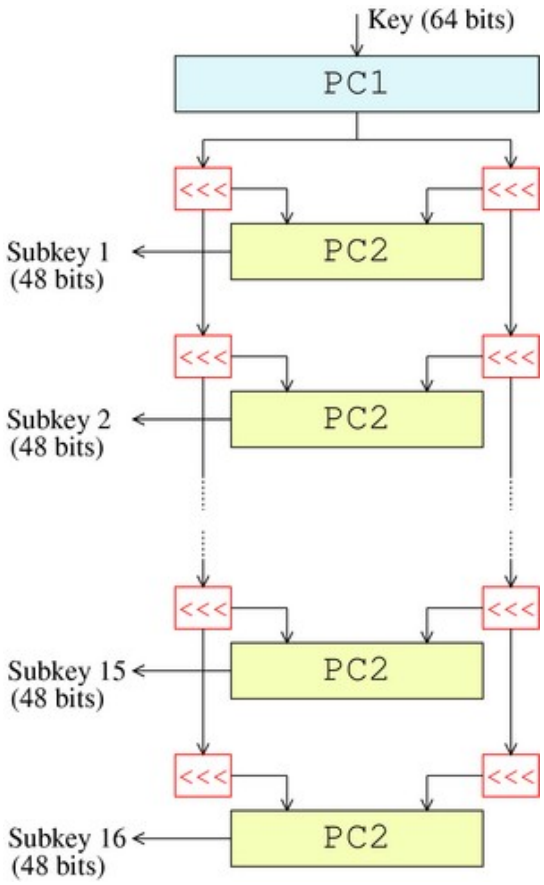
A) Symmetric-Key Cryptography

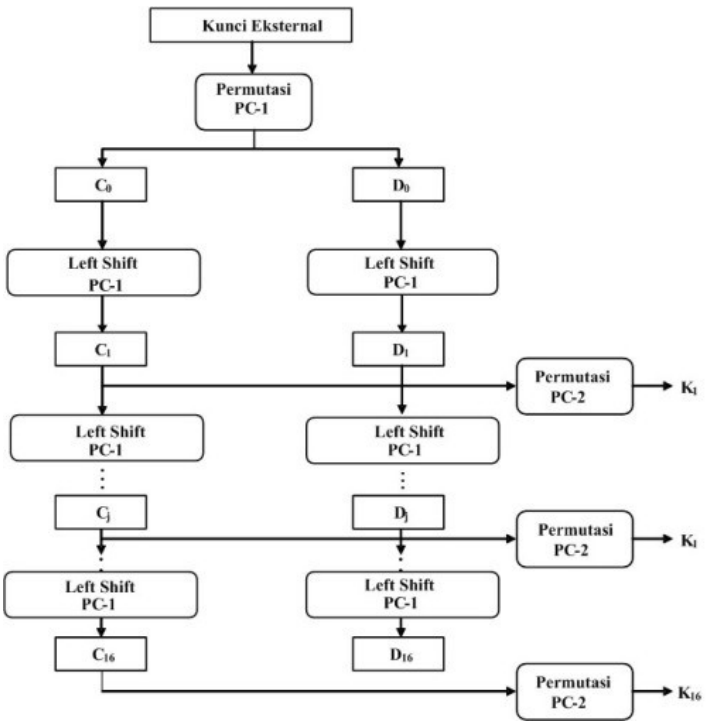
Algoritma simetris atau sering disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Dimana pada algoritma aliran, proses penyandiannya akan beriorientasi pada satu bit/byte data. Sedangkan pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit/byte data (per blok).

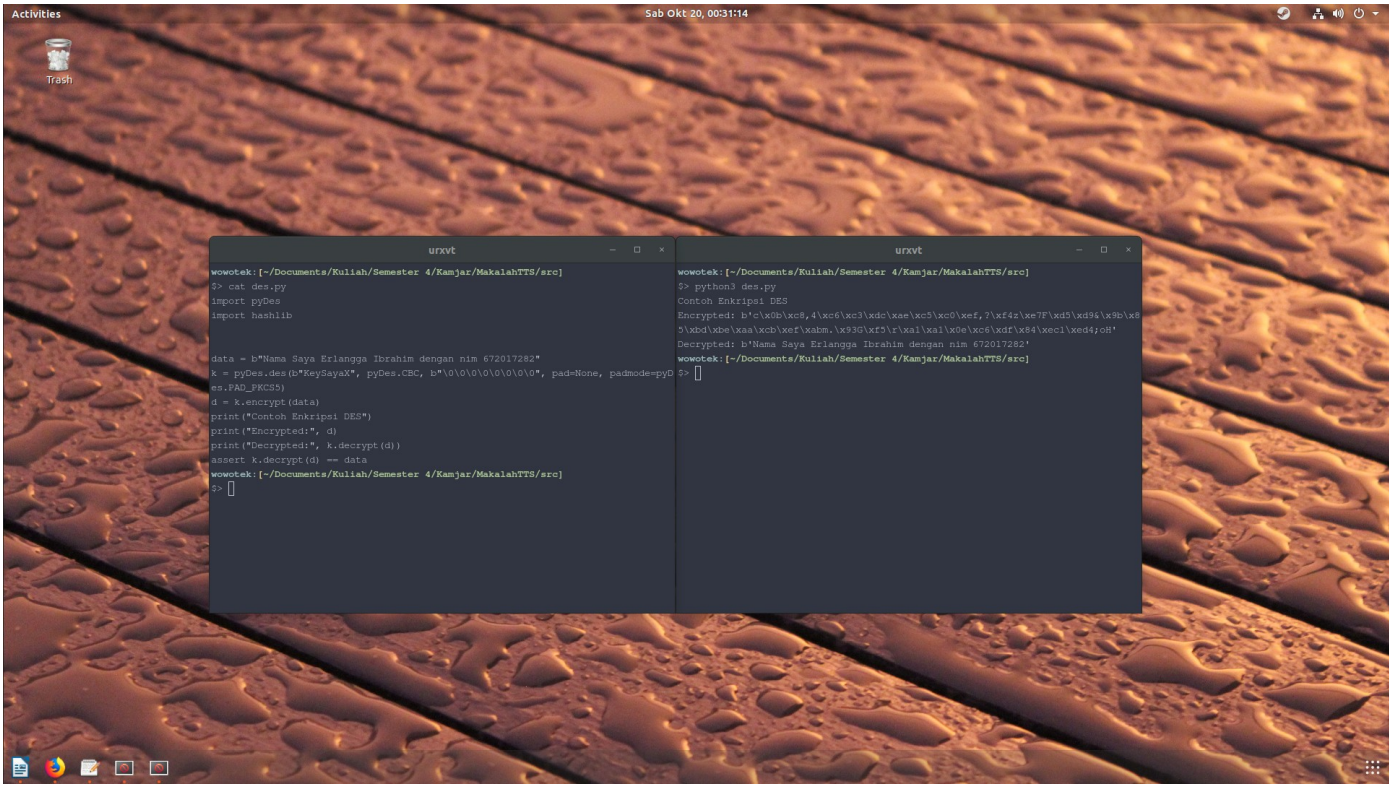
- **Data Encryption Standard (DES)**

  DES merupakan algoritma enkripsi yang dikembangkan oleh NIST (National Institute of Standards and Technology) sebagai standar pengolahan informasi Federal AS. Secara umum, Data Encryption Standard (DES) terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit dan deskripsi data 64 bit, dimana satu kelompok saling berinteraksi satu dengan yang lainnya.
  Data dienkripsi dalam blok-blok 64 bit menggunakan kunci 56 bit, DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk lama block cipher dengan tahapan pemakaian kunci yang sama untuk deskripsinya.

  DES, atau juga dikenal sebagai Data Encryption Algorithm (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Sejarahnya DES dimulai dari permintaan pemerintah Amerika Serikat untuk memasukkan proposal enskripsi. DES memiliki sejarah dari Lucifer1, enkripsi yang dikembangan di IBM kala itu. Horst Feistel merupakan salah satu periset yang mula-mulA mengembangkan DES ketika bekerja di IBM Watson Laboratory di Yorktown Heights, New York. DES baru secara resmi digunakan oleh pemerintah Amerika Serikat (diadopsi oleh National Bureau of Standards) di tahun 1977. Ia dikenal sebagai Federal Information Processing Standard 46 (FIPS PUB46).

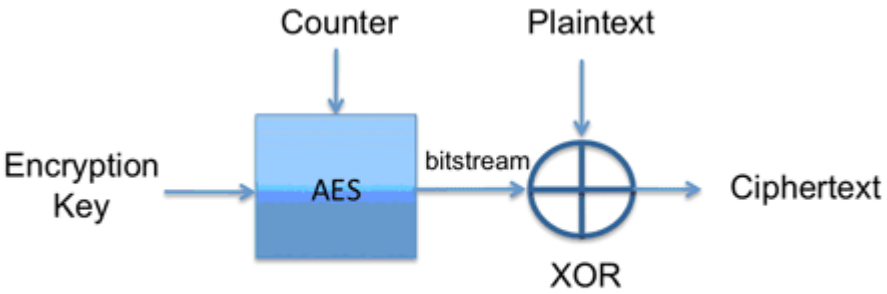


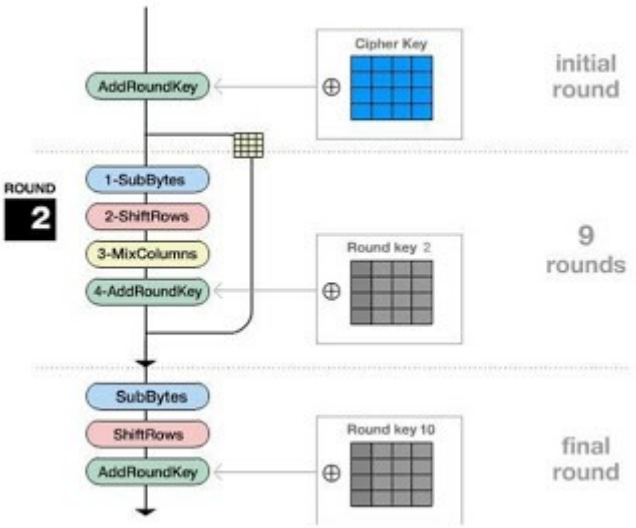


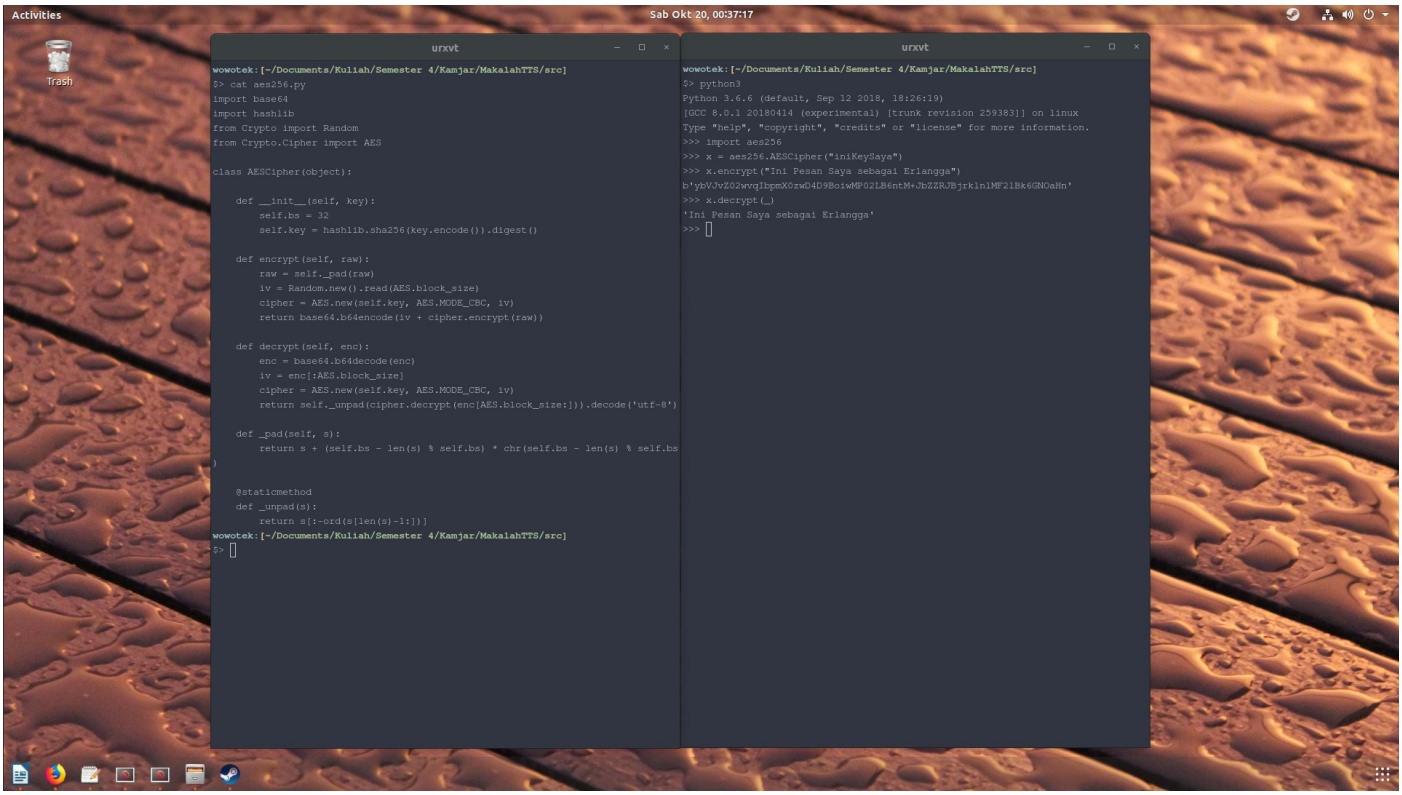


- **Advanced Encryption Standard (AES)**

  AES (Advanced Encryption Standard) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya. Keamanan merupakan faktor terpenting dalam evaluasi (minimal seaman triple DES), yang meliputi ketahanan terhadap semua analisis sandi yang telah diketahui dan diharapkan dapat menghadapi analisis sandi yang belum diketahui. Di samping itu, AES juga harus dapat digunakan secara bebas tanpa harus membayar royalti, dan juga murah untuk diimplementasikan pada smart card yang memiliki ukuran memori kecil. AES juga harus efisien dan cepat (minimal secepat Triple DES) dijalankan dalam berbagai mesin 8 bit hingga 64 bit, dan berbagai perangkat lunak. DES menggunakan stuktur Feistel yang memiliki kelebihan bahwa struktur enkripsi dan dekripsinya sama, meskipun menggunakan fungsi F yang tidak invertibel. Kelemahan Feistel yang utama adalah bahwa pada setiap ronde, hanya setengah data yang diolah. Sedangkan AES menggunakan struktur SPN (Substitution Permutation Network) yang memiliki derajat paralelisme yang lebih besar, sehingga diharapkan lebih cepat dari pada Feistel.



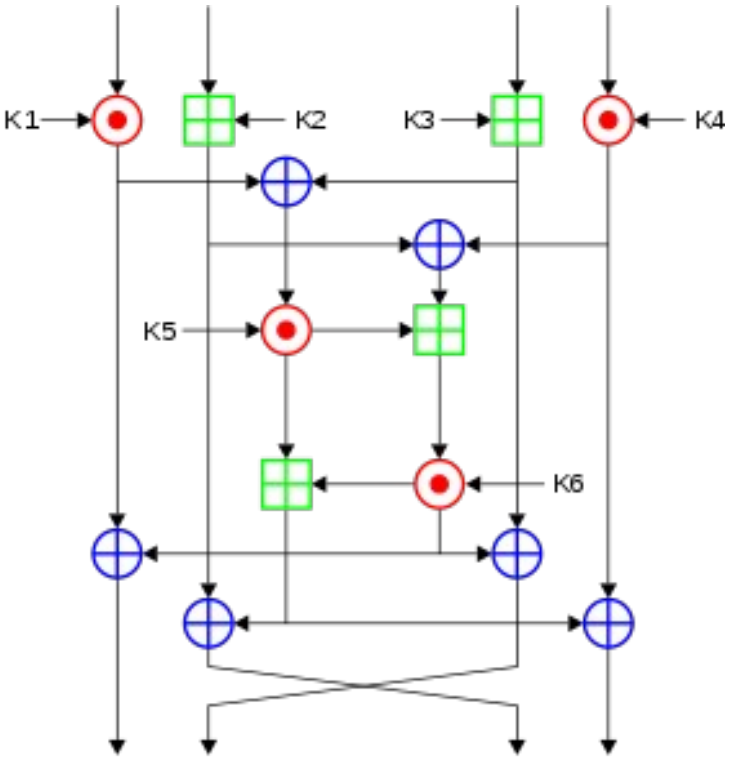


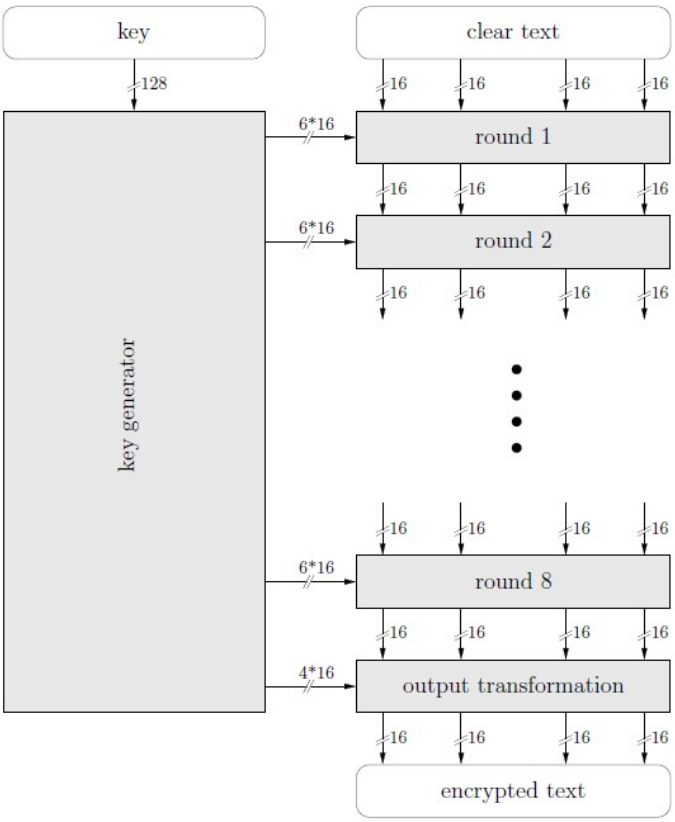


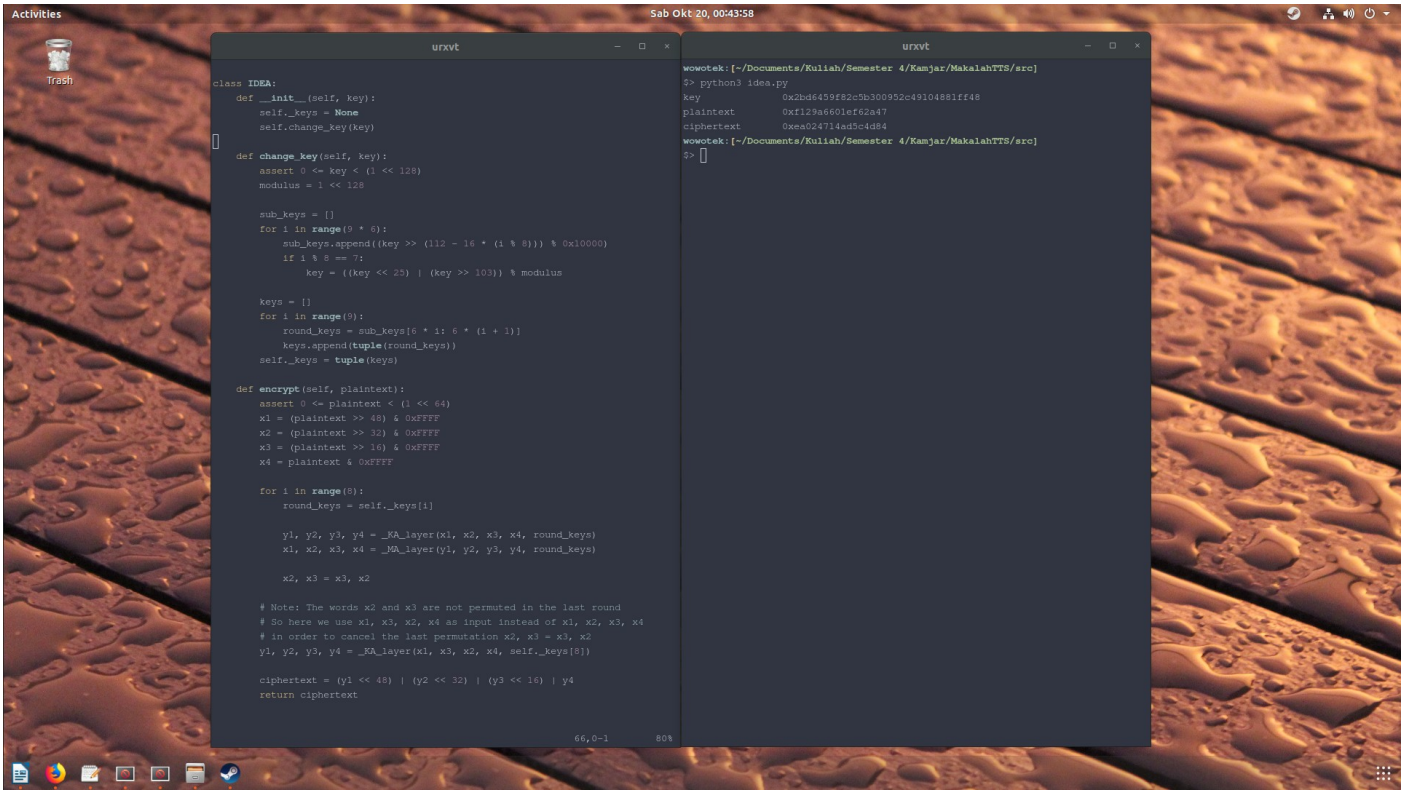
- **International Data Encryption Algorithm (IDEA)**

  IDEA (International Data Encryption Algorithm) merupakan algoritma simetris yang beroperasi pada sebuah blok pesan terbuka dengan lebar 64-bit. Dan menggunakan kunci yang sama , berukuran 128-bit, untuk proses enkripsi dan dekripsi. Pesan rahasia yang dihasilan oleh algoritma ini berupa blok pesan rahasia dengan lebar atu ukuran 64-bit

Pesan dekripsi menggunakan blok penyandi yang sama dengan blok proses enkripsi dimana kunci dekripsinya diturunkan dari dari kunci enkripsi. Algoritma ini menggunakan operasi campuran dari tiga operasi aljabar yang berbeda, yaitu XOR, operasi penjumlahan modulo 216 dan operasi perkalian modulo (216 + 1) .







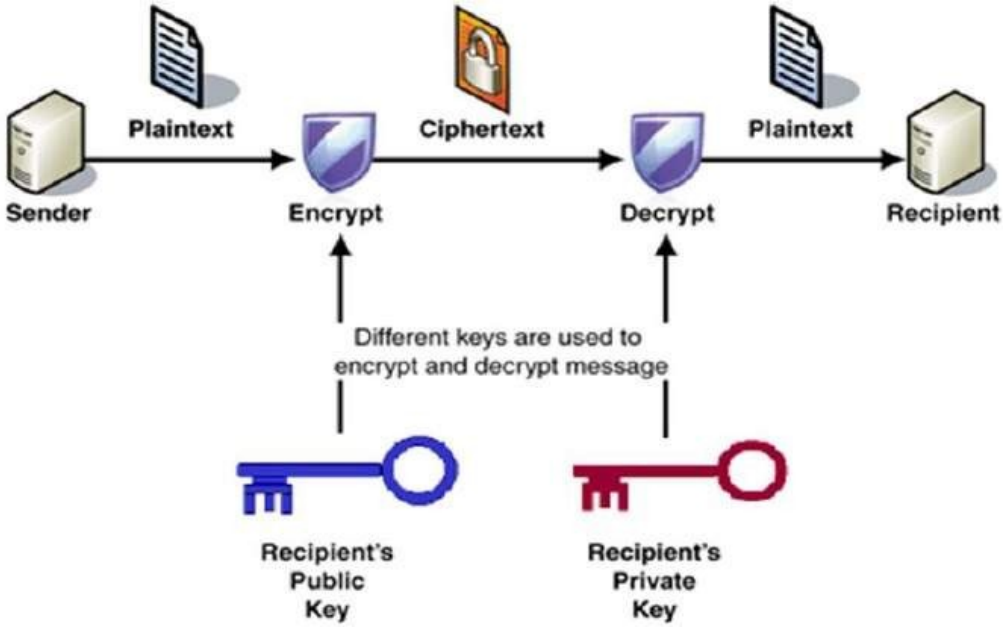
B) Public-Key Cryptography

Sampai akhir tahun 1970, hanya ada sistem kriptografi simetri. Karena sistem kriptografi simetri menggunakan kunci yang sama untuk enkripsi dan dekripsi, maka hal ini mengimplikasikan dua pihak yang berkomunikasi saling mempercayai. Kedua pihak harus menjaga kerahasiaan kunci (sehingga, junci enkripsi/dekripsi disebut juga secret key)

- **RSA**

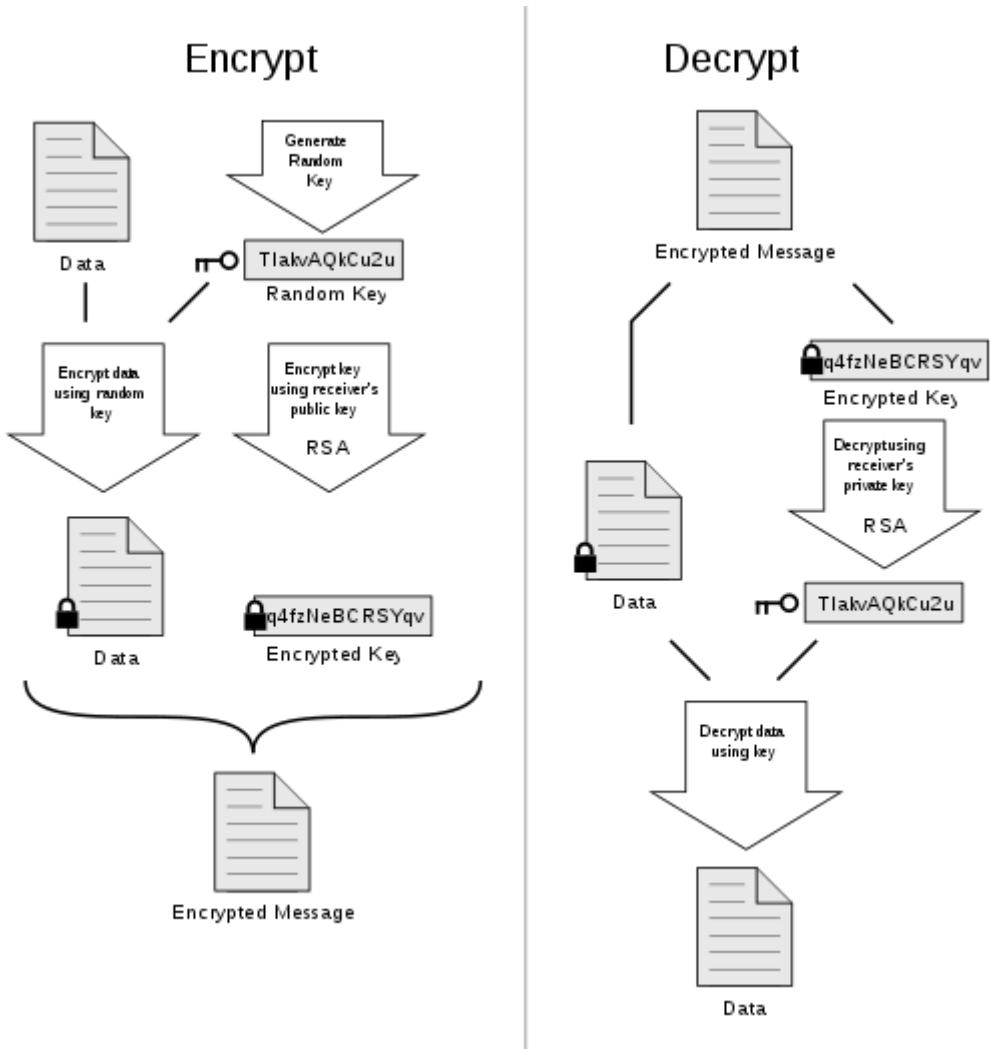
  Algoritma RSA merupakan salah satu algoritma public key yang populer dipakai dan bahkan masih dipakai hingga saat ini. Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya.

  Algoritma ini dinamakan sesuai dengan nama penemunya, Ron Rivest, Adi Shamir dan Adleman(Rivest-Shamir-Adleman) yang dipublikasikan pada tahun 1977 di MIT, menjawab tantangan yang diberikan algoritma pertukaran kunci Diffie Hellman.



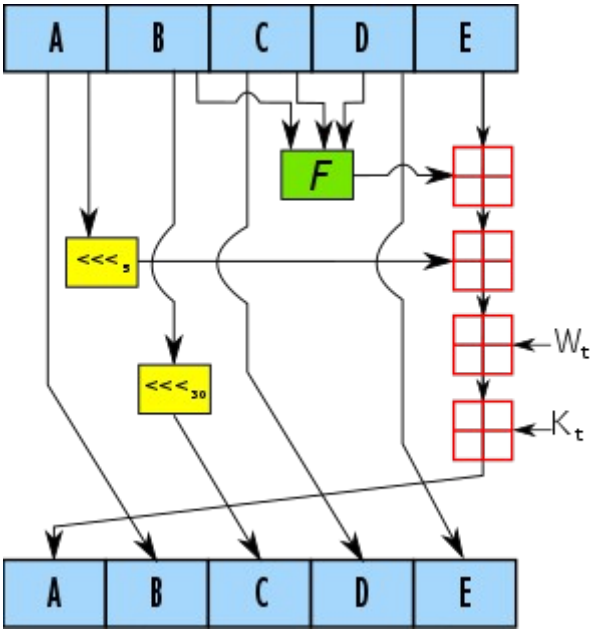
- **PGP**

PGP (Pretty Good Privacy) adalah Suatu metode program enkripsi informasi yang memiliki tingkat keamanan cukup tinggi bersifat rahasia dengan menggunakan “Private-Public Key” sebagai dasar autentifikasinya sehingga jangan sampai dengan mudah diketahui oleh orang lain yang tidak berhak. PGP dikembangkan oleh Phill Zimmermann pada akhir tahun1980. Program yang dibuat oleh Phill Zimmerann memiliki 2 versi yaitu “USA Version “ dan “International Version”. PGP versi USA hanya dapat digunakan di wilayah USA dan oleh warganegara USA saja. PGP versi USA ini menggunakan algoritma RSA (yang telah menjadi hak paten) dalam enkripsinya. Sedangkan versi internasional menggunakan algoritma MPILIB yang diciptakan khusus oleh Phill Zimmermann sendiri. PGP Versi internasional bisa digunakan oleh seluruh dunia.



- **SHA 1**

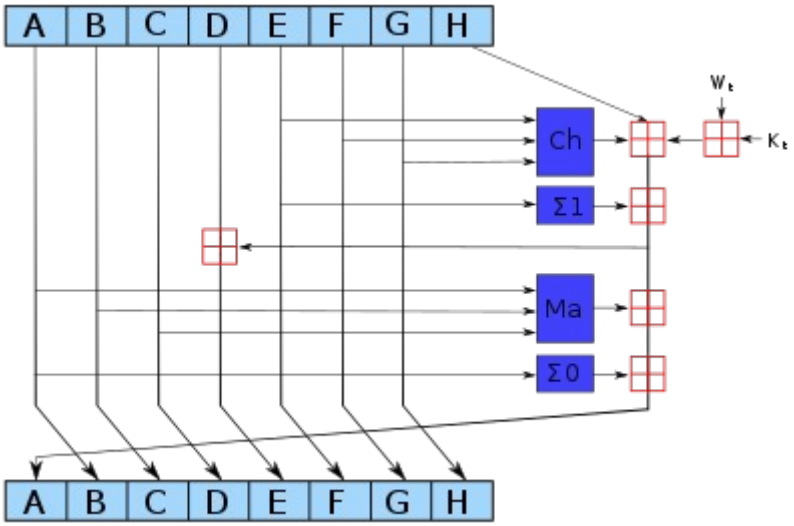
  SHA1 atau Secure Hash Algorithm 1 merupakan salah satu algoritma hashing yang sering digunakan untuk enkripsi data. Hasil dari sha1 adalah data dengan lebar 20 byte atau 160 bit, biasa ditampilkan dalam bentuk bilangan heksadesimal 40 digit.

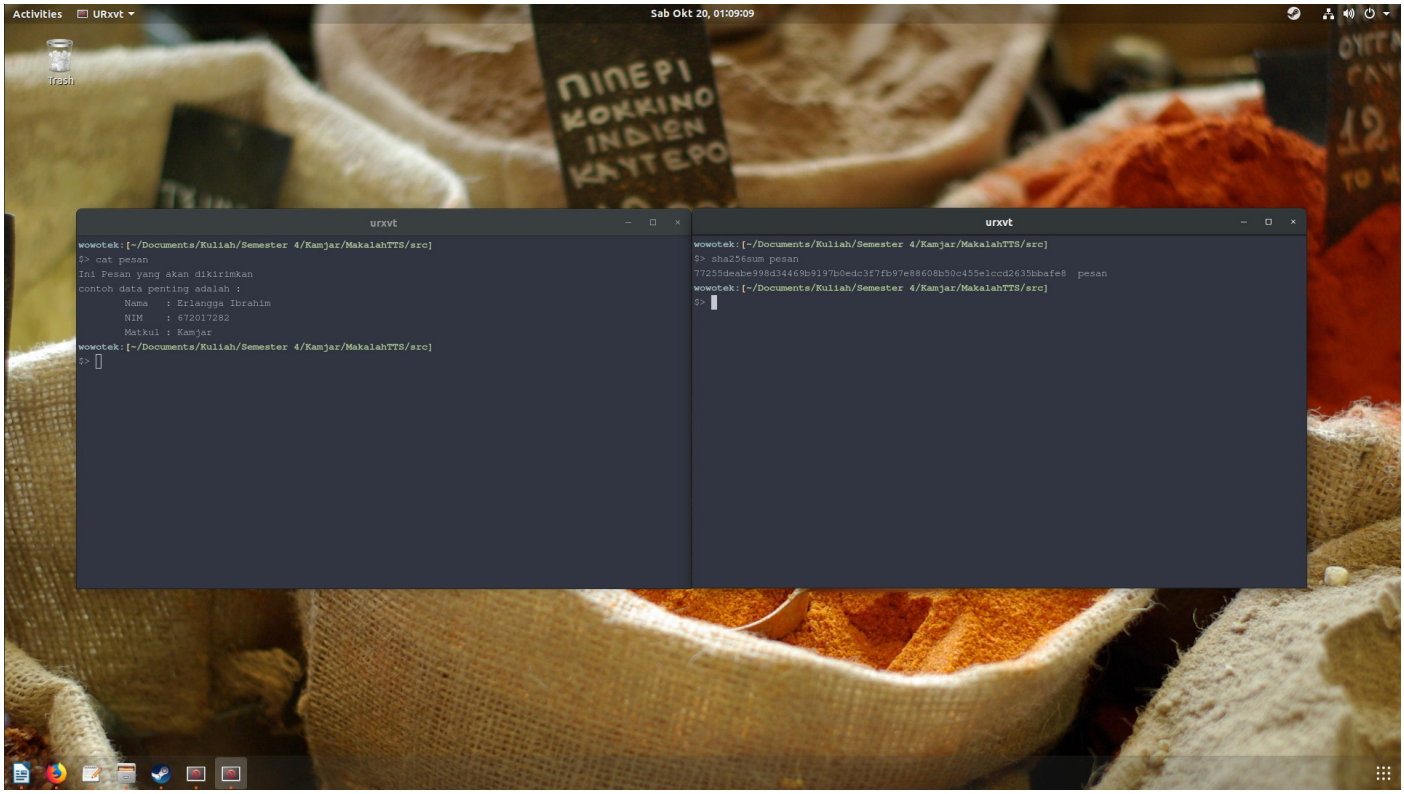


- **SHA 2**

  Algoritma SHA-2 merupakan pengembangan dari algoritma sha-1 yang memuat banyak perubahan. Algoritma ini didesain oleh National Security Agency (NSA) of United States dan dipublikasikan pada tahun 2001 oleh NIST sebagai standar bagi pemrosesan informasi federal bagi Amerika Serikat atau yang biasa disebut *Federal Information Processing Standard (FIPS).*

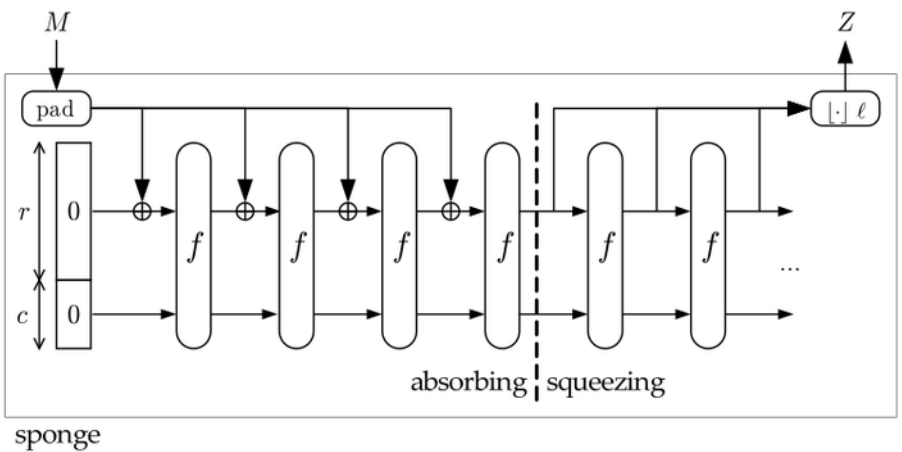
  Algorima SHA-2 ini terdiri dari beberapa algoritma berdasarkan panjang bit yang digunakan/dihasilkan sebagai nilainya yaitu SHA-224, SHA-256, SHA-384, SHA-512.





- **SHA 3**

  SHA-3 ini dikenal sebagai Keccak yang dirancang oleh Guido Bertoni, Joan Daemen, Peeters Michael, dan Gilles Van Assche. SHA-3 atau Keccak ini merupakan pemenang dari kompetisi fungsi hash NIST. SHA-3 ini menggunakan sponge construction dimana blok pesan XOR ke dalam bit awal state yang kemudian di lakukan permutasi, dimana input ke state hash pada tingkatan tertentu akan menghasilkan output yang mempunyai tingkatan yang sama. SHA-3 terdiri dari 5 x 5



array 64-bit kata, 1600 bit total. Belum ada standar untuk fungsi SHA-3 ini termasuk sistem enkripsi otentik dan pohon hash.